Examiner's Amendment and Statement of Reasons for Allowance

1. This action is responsive to Applicant's amendment filed September 29, 2009.

Examiner's Amendment

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Jeff Limon, Registration Number 45,418, on October 27, 2009 for obviating any potential 101 issues and put the claims in condition for allowance.

The application has been amended as follows:

Claim 1. (Currently Amended) An electronic device network, the network comprising:

a plurality of servers;

a plurality of electronic devices communicatively coupled to at least one of the plurality of servers, each of the electronic devices being adapted to employ at least one of a plurality of update agents resident in the electronic device, wherein the update agent employed is selected to correspond to a type of update information received by the electronic device from the at least one of the plurality

of servers, wherein the selected update agent processes the received update information to modify a first version of one of software and firmware in the electronic device to a second version, and wherein the electronic device is also adapted to provision the plurality of update agents with parameters and data used to facilitate update operations in the electronic device, wherein the electronic device comprises random access memory and non-volatile memory, wherein the non-volatile memory comprises a plurality of components, the plurality of components comprising at least one of the following: an update application loader, the plurality of update agents, firmware, an operating system (OS), and provisioned data; and wherein the provisioned data comprises update agent provisioning information and a number assignment module;

wherein the electronic device comprises a provisioned data unit adapted to store information related to an end-user's electronic device subscription, and wherein the provisioned data unit may be programmed during number assignment module programming activity;

wherein the number assignment module programming activity comprises at least one of over-the-air service provisioning (OTASP) activity and over-the-air parameter administration (OTAPA) activity; and

a database in each of the plurality of electronic devices for accessing the plurality of provisioned update agents in a corresponding electronic device.

Claim 2. (Canceled)

Claim 3. (Previously Presented) The network according to claim 1, wherein the network comprises at least one of an update server, and a plurality of generators, wherein the generators are adapted to generate updates able to be processed by at least one provisioned update agent in the electronic device, and wherein the update server is adapted to store updates accessible by the plurality of servers.

Claim 4. (Canceled)

Claim 5. (Canceled)

Claim 6. (Currently Amended) The network according to claim 1 [4], wherein the provisioned data unit is adapted to store at least one of update agent related provisioning information, a universal resource locator of a server used to retrieve updates, and a security key used to authenticate server messages.

Claim 7. (Currently Amended) The network according to claim 1 [4], wherein each of the plurality of update agents has a corresponding entry in the provisioned data unit.

Claim 8. (Previously Presented) The network according to claim 1, wherein one of the plurality of update agents is designated a primary update agent and another of the plurality of update agents is designated as a secondary update agent, and wherein the primary update agent is used to perform updates during one of power up and reboot of the electronic device and the secondary update agent is used to perform updates not requiring electronic device rebooting.

Claim 9. (Original) The network according to claim 1, wherein the electronic device is adapted to display a list of available update agents to an end-user and solicit selection of an update agent to be used to update at least one of software and firmware.

Claim 10. (Previously Presented) The network according to claim 1, wherein the electronic device is adapted to invoke an update agent based upon an update currently being processed provided that the update agent is provisioned in the electronic device.

Claim 11. (Previously Presented) The network according to claim 1, wherein the electronic device may execute an update application loader on reboot, and wherein the update application loader is adapted to invoke a boot initialization code before determining to update the electronic device.

Claim 12. (Previously Presented) The network according to claim 1, comprising update agent provisioning information stored in the electronic device, the update agent provisioning information comprising at least one of the following: a device server URL, an index to the database for accessing the plurality of provisioned update agents, a security key, and electronic device related information, wherein the device server URL provides references to servers hosting updates to be downloaded, and wherein the updates are compatible with update agents currently available and provisioned in the electronic device.

Claim 13. (Previously Presented) The network according to claim 12, wherein the index to the database for accessing the plurality of provisioned update agents provides an index value used to compute an address location of a provisioned update agent, and wherein the index to the database for accessing the plurality of provisioned update agents provides an index to a table containing an address for an update agent in non-volatile memory the electronic device.

Claim 14. (Previously Presented) The network according to claim 12, wherein the security key is used to authenticate updates during download of updates and during update activity, wherein a separate security key is employed to authenticate updates by a download agent and by the update agent, and wherein the security key is employed for at least one of the following: secure communication, encryption, and decryption of data and messages during communication with external systems.

Claim 15. (Previously Presented) The network according to claim 1, wherein the database for accessing the plurality of provisioned update agents in the electronic device comprises an update agent table resident in non-volatile memory, the update agent table containing references to a plurality of update agents currently available and provisioned in the electronic device, the update agent table associating update agent names, update agent address locations, types of updates that the update agents are adapted to process, and provisioning status of the update agents for all available update agents in the electronic device.

Claim 16. (Previously Presented) The network according to claim 1, wherein the electronic device comprises at least one of a plurality of mobile electronic devices, and wherein the plurality of mobile electronic devices comprise at least one of the following: a mobile cellular phone handset, a personal digital assistant, a pager, an MP3 player, and a digital camera.

Claim 17. (Currently Amended) A method employing a plurality of update agents in an electronic device in an electronic device network, the method comprising:

communicatively coupling a plurality of electronic devices to at least one of a plurality of servers;

selecting at least one of a plurality of update agents resident in the electronic device to modify a first version of one of software and firmware in the electronic device to produce an updated version, wherein each of the plurality of update

agents is arranged to process a corresponding type of update information received from the at least one of a plurality of servers; ~~and~~

provisioning the plurality of update agents with parameters and data used to facilitate update operations in the electronic device, wherein a database is used for accessing the plurality of provisioned update agents;

storing information related to a provisioned data unit for an end-user's electronic device subscription;

programming the provisioned data unit during number assignment module programming activity, wherein the number assignment module programming activity comprises at least one of the following: over-the-air service provisioning (OTASP) activity and over-the-air parameter administration (OTAPA) activity.

Claim 18. (Previously Presented) The method according to claim 17, comprising generating updates able to be processed by at least one provisioned update agent in the electronic device and storing updates in an update server.

Claim 19. (Canceled)

Claim 20. (Canceled)

Claim 21. (Previously Presented) The method according to claim 17 [19], wherein the programming comprises storing update agent related provisioning information, a universal resource locator of a server used to retrieve updates, and a security key used to authenticate server messages.

Claim 22. (Previously Presented) The method according to claim 17 [19], comprising providing each update agent an entry in a provisioned data unit.

Claim 23. (Previously Presented) The method according to claim 17, comprising:

designating a primary update agent and a secondary update agent;

using the primary update agent to perform updates during one of the following: power up and reboot of the electronic device; and

using the secondary update agent to perform updates not requiring electronic device rebooting.

Claim 24. (Previously Presented) The method according to claim 17, comprising:

displaying a list of available update agents to an end-user; and

soliciting selection of an update agent to be used to update at least one of software and firmware.

Claim 25. (Previously Presented) The method according to claim 17, comprising invoking an update agent based upon an update currently being processed provided that the update agent is provisioned in the electronic device.

Claim 26. (Previously Presented) The method according to claim 17, comprising executing an update application loader on reboot of the electronic device and invoking a boot initialization code before determining to update the electronic device.

Claim 27. (Previously Presented) The method according to claim 17, comprising:

storing update agent provisioning information in the electronic device; and

hosting updates to be downloaded with update agents provisioned in the electronic device.

Claim 28. (Previously Presented) The method according to claim 17, comprising determining an address location of a provisioned update agent via the database for accessing the plurality of provisioned update agents, wherein determining comprises one of computing and accessing an entry in a table.

Claim 29. (Previously Presented) The method according to claim 17, comprising:

authenticating updates during download of the updates and during update activity, using a security key;

employing a separate security key to authenticate updates by a download agent and by the at least one of a plurality of update agents; and

employing the security key for at least one of the following: secure communication, encryption, and decryption of data and messages, during communication with external systems.

Claim 30. (Previously Presented) The method according to claim 17, comprising mapping at least one of the following: update agent names, update agent address locations, types of updates that the update agents are adapted to process, and provisioning status of the update agents, for all available update agents in the electronic device.

Claim 31. (Previously Presented) The method according to claim 17, wherein the electronic device comprises at least one of the following: a plurality of mobile electronic devices, and wherein the plurality of mobile electronic devices comprise at least one of a mobile cellular phone handset, a personal digital assistant, a pager, an MP3 player, and a digital camera.

Claim 32. (Currently amended) An electronic device operable in an electronic device network, the electronic device comprising:

non-volatile memory comprising a first version of code;

communication circuitry for receiving, from at least one server in the electronic device network, update information having an associated type;

code resident in and executable by the electronic device, the code comprising a plurality of provisioned update agents selectable to cause processing of a corresponding type of received update information, to update a related code portion of the first version of code to an updated version, wherein a database in the electronic device enables accessing of the plurality of provisioned update agents;

wherein the processing modifies the related code portion of the first version of code to produce the updated version;

wherein the electronic device comprises random access memory and non-volatile memory, wherein the non-volatile memory comprises a plurality of components, the plurality of components comprising at least one of the following: an update application loader, the plurality of update agents, firmware, an operating system (OS), and provisioned data, and wherein the provisioned data comprises update agent provisioning information and a number assignment module;

wherein the electronic device comprises a provisioned data unit adapted to store information related to an end-user's electronic device subscription, and wherein the provisioned data unit may be programmed during number assignment module programming activity;

wherein the number assignment module programming activity comprises at least one of over-the-air service provisioning (OTASP) activity and over-the-air parameter administration (OTAPA) activity; and

wherein a provisioned update agent is selected to perform an update based upon the type of the received update information.

Claim 33. (Previously Presented) The electronic device according to claim 32 wherein the communication circuitry comprises a cellular network interface.

Claim 34. (Previously Presented) The electronic device according to claim 32 wherein the update information comprises an update package.

Claim 35. (Previously presented) The electronic device according to claim 32 wherein a portion of the non-volatile memory comprises provisioned data received from at least one of the plurality of servers.

Claim 36. (Previously presented) The electronic device according to claim 35 wherein the provisioned data comprises at least one entry corresponding to one of the plurality of provisioned update agents.

Claim 37. (Canceled)

Claim 38. (Previously Presented) The electronic device according to claim 35 wherein provisioned data comprises a universal resource locator of a server on which a corresponding type of update information is stored.

Claim 39. (Previously Presented) The electronic device according to claim 35 wherein provisioned data comprises security information enabling update of the related code portion.

-- The End --

Examiner's Statement of Reason(s) for Allowance

3. Claims 1, 3, 6-18, 21-36, 38-39 are allowed.

4. The following is an examiner's statement of reasons for allowance:
The prior arts of record: **Aghera** et al., teaches an architecture for over the air management of software on a wireless device includes a software architecture supporting software patches, including secure downloading of software from a data network and robust installation of the same on the wireless device. Using this architecture, a network operator can notify a mobile device user about the software upgrade and send the upgrade to the mobile device over the air. Remote management of DSP software on mobile phones in GSM or GPRS networks uses an efficient installation algorithm with an error recovery mechanism. **McGuire** et al., teaches a method and system for downloading software update data for installing a revised software product on a client computer minimizes the amount of update data to be transmitted over the network by downloading only those files needed to put the client computer in the state for installing the product. In the beginning of the downloading process, the client computer obtains from a setup server an initial setup package that includes a setup program and a list of files required for installing the software product. The setup program running on the client computer then determines whether some current or earlier versions of those files required for installation already exist on the client computer, and compiles a request list of files needed for updating the client computer. **Kikinis**, teaches an automatic recovery system for a network appliance features a watchdog processor that monitors operation of the appliance and initiates reboot as necessary. A primary and a secondary boot partition are provided in the system, in

some embodiments on the same mass storage device, and in other embodiments on a different mass storage device. In the event reboot is unsuccessful from the primary boot partition, reboot is initiated from the secondary boot partition.

Lee Kyu-Woong et al., teaches a computer-implemented method for updating a plurality of software components disposed on a plurality of networked devices, the plurality of networked devices being interconnected in a computer network. The method includes ascertaining from a database first update parameters associated with a first networked device of the plurality of networked devices. The method also includes sending via the network the first update parameters to a first local update agent disposed at the first networked device. The method further includes obtaining, using the first local update agent and the first update parameters, a first update file for updating software in the first networked device. Additionally, the method includes updating, using the first local update agent and the first update file, the software in the first networked device. **Rao**, teaches a method for updating at least one of firmware, software, device components, and device configuration in an electronic device. The method and apparatus may employ at least one update agent or a plurality of update agents. An electronic device supporting multiple update agents may be adapted to prompt and facilitate an end-user to select at least one of the update agents to process update information contained in at least one update. The electronic device may also be adapted to prompt and facilitate an end-user to apply a particular update agent to update at least one of firmware, software, device components, device configuration, device information, and device parameters. **Meyerson**, teaches a method of updating computer software includes downloading software update information through a network, such as the Internet, to a user's computer. The

download is preferably done periodically and automatically. If available, a criticality check program identified in the software update information is then automatically downloaded and executed to determine the configuration of the user's computer. The criticality and applicability of available software updates are evaluated by the criticality check program in light of the specific software and/or hardware configuration of the user's computer. The software updates may then be downloaded and installed automatically, if previously authorized by the user, by comparing the criticality of the updates to the user, as determined by the criticality check program, to stored user preference information specifying a user criticality threshold. Software updates determined to be more critical than the user criticality threshold are installed automatically and the user is notified of the availability of less critical updates. **Ogawa**, teaches an update client sends to an update server which is connected to the update client via a communication line, identification information of a driver and firmware which are included in a disk array system, and identification information of an error event which has occurred in the disk array system. The update server determines whether update of the driver and the firmware is necessary or not in accordance with a combination of the supplied identification information of the driver, the firmware, and the error event. In a case where it is determined that update is necessary, the update server sends to the update client, update data corresponding to the combination of the supplied identification information of the driver, the firmware, and the error event. **Lee, Cheng-Yin** et al., teaches location update messages for a mobile node can be made interceptible by routers which form tunnels for communication with the mobile node. A correspondent agent intercepts a Binding Update with a Router Alert and binds the address of the mobile node with a care of address for

the mobile node provided in the Binding Update. The correspondent agent will thereafter intercept messages from its correspondent host destined for the mobile node and redirect them to the care of address thereby bypassing the home agent of the mobile node. A border router intercepts a Registration Request with Router Alert and binds the address of the mobile node with a care of address for the mobile node. If a binding existed previously, then the border router terminates the Request. **Yang** et al., teaches an apparatus, system and method are provided for OTA downloading, configuring and updating application programs stored in a memory of mobile communication device. The apparatus and method include a number of downloadable or "built-in" application-based programs that efficiently perform the following: customizing services from various service providers via internet or call centers; downloading new applications and updating existing applications via short, wireless messages from application servers to the mobile device; notifying service providers through internet protocol between wireless application servers and service providers; uploading and registering new applications to wireless application servers from developers through the internet; and parsing short, wireless messages from messaging centers using application managers to distinguish between command messages for applications and regular text messages. **Heisey** et al., teaches a tool for replacing a code image in an embedded device including a control program for issuing device commands in order to replace a code image within the embedded device. A monitoring program, operating asynchronously with respect to the control program, generates event indications in response to detecting a change in an attribute associated with the embedded device. The disclosed monitoring program issues device commands and receives event indications. Separate threads of control are used for monitoring

and controlling the device being upgraded, and each step of the upgrade process is abstracted as a device independent command. The disclosed system further uses a state machine to keep track of where the device is in the upgrade process. **Cole**, teaches a system and method are provided for determining whether to provide a software program update to one of a plurality of client processors. Each client processor has a copy of at least one of a plurality of client software programs. A respective set of system configuration attributes are sent from each client processor and stored in an administration server processor. Each set of system configuration attributes is transmitted to a selection server processor. A respective update recognizer program and software program update corresponding to each respective one of the plurality of client software programs are next sent to the administration server processor. Each client processor executes at least one of the update recognizer programs to issue a notification indicating whether the corresponding software program update is applicable. New arts made of record: US Patent No. 6,990,660, by **Moshir** et al., teaches Methods, systems, and configured storage media are provided for discovering software updates, discovering if a given computer can use the software update, and then updating the computers with the software as needed automatically across a network without storing the updates on an intermediate machine within the network. Furthermore, when a failure is detected, the rollout is stopped and the software can be automatically removed from those computers that already were updated. The software update can be stored originally at an address that is inaccessible through the network firewall by intermediately uploading the software update to an update computer which is not a part of the network but has access through the firewall, which is then used to distribute the update. US 2003/0055931 by **Craovo De**

Almeida et al., teaches an agent obtains data from a device by receiving a plug-in containing system calls for obtaining the data from the device, loading the plug-in into the agent, obtaining the data from the device using the system calls, and transmitting the data over an external network using one or more of a plurality of protocols. The data is provided to a client by formatting the data, and making the formatted data accessible to a client via the external network. US Patent No. 6,553,375 by **Huang** et al., teaches a novel management system for selectively distributing applications and databases from a server computer to a plurality of intermittently connected handheld devices. The applications and databases to be downloaded and deleted are first selected from an application list maintained by handheld devices. After established a connection with the server computer, the application list of selected applications is copied to the server computer which maintains an access control list indicating which applications are permitted to be downloaded to which handheld devices. The server computer examines the application list and the access control list to determine which applications are both selected and are authorized for use by the handheld device. US Patent 6,249,817 by **Nakabayashi** et al., teaches an user I/F unit transmits an instruction given by a user to an access management unit and displays data on a monitor. The access management unit transfers requirements to a communication control unit and a data management unit in response to the instruction from the user, transfers data from a communications host to the data management unit, and outputs data from a database to the user I/F unit. The data management unit writes data into the database and reads storage data from the database in response to the requirement from the access management unit. Data

transmitted from the communications host are sorted out according to communication services and stored in the database. The communication control unit translates the requirement from the access management unit to a menu number representing each communication service available from the communications host or a command and sends the translated requirement to a communication I/F unit. US Patent No. 6,282,709 by **Reha** et al., teaches a method and apparatus for checking/updating existing software on a user's computer utilizes a graphical user interface (GUI). The GUI enables the user, without knowing what software exists on the computer, to download a text file from a remote server and check whether the software on the remote server is contained on the user's computer. The user can also download and automatically install a new or updated program via the GUI. US Patent No. 6,636,958 by **Abboud** et al., teaches a method and hard disk configuration for accommodating different sizes of applications during an automatic re-provisioning of an appliance server. The disk drive of the appliance server is partitioned with a system partition, a network operating system (NOS) partition, a float partition, and an images partition. The float partition is utilized to provide additional space to the NOS partition and the images partition, when required. A re-provisioning utility is provided, which initiates both a create image utility and an apply image utility, whereby an image file of a current application and associated operating system is created and a stored image file of a second application is installed on the appliance server. When the apply image utility is initiated, the NOS partition is dynamically extended into the float partition server if the second application requires more space than is provided in the NOS partition. US Patent No. 6,690,390 by **Walters** et al., teaches a computer system and method for

performing a task within an application from within an on-line help information display. Thus the on-line help information displayed by the computer system may include user selectable elements which enable the user to complete portions or all of a task directly from the on-line help window, e.g., without requiring the user to search for this functionality in menus or toolbars within the application. The user may launch the application and then select on-line help information associated with performing a task within the application. In response to this user input, the computer may display on-line help information associated with the application. The displayed on-line help information may include various help information that specifies a recipe for performing the task, e.g., the information may guide the user through a series of steps to perform the task in the application. The displayed on-line help information may include one or more user selectable elements. In response to the user selecting a user selectable element, the application may perform at least a portion of the task within the application. Thus the user can perform a portion or all of a task by selecting an element or item directly from the on-line help information window. US Patent No. 6,546,419 by **Humpleman** et al., teaches method and system for performing a service on a home network having a plurality of home devices connected thereto, by: connecting a client device to the home network for displaying a user interface; executing a software agent on the client device for obtaining selection information for the network devices and displaying the selection information on a user interface displayed on the client device; selecting a first home device connected to the network from the user interface being displayed on the client device; reading first capabilities data for the first home device, where the first capabilities data includes information in a structured format for identifying the capabilities of the

first home device; reading second capabilities data for a second home device connected to the network, where the second capabilities data includes information in the structured format for identifying the capabilities of the second home device; comparing the first and second capabilities data of the first and second home devices, respectively; selecting the second home device from the user interface displayed on the client device; and sending control and command data from the client device to the first and second home devices to cause the first and second home devices to communicate with each other to perform the service. And US Patent No. 6,970,698 by **Majmundar** et al., teaches a central host performs an automated method of updating multiple remote devices. In one embodiment, the host recognizes a predetermined download time and, in advance of the download time, transmits a calendar update to multiple remote devices. The calendar update includes the download time, and the remote devices may utilize the download time to set calendar reminders for entering an active state. Within a short time after reaching the download time, the host pushes download data to the remote devices by broadcasting the download data. In one aspect, the host may receive message acknowledgements from remote devices in response to a first calendar update, and the host may automatically transmit additional calendar updates to any remote devices that did not receive the first calendar update. However, none of them, taken alone or in combination, teaches the features in such a manner as recited in independent claims 1, 17, and 32.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chih-Ching Chow whose telephone number is 571-272-3693. The examiner can normally be reached on 8:00am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Wei Zhen can be reached on 571-272-3708. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Chih-Ching Chow/
Examiner, Art Unit 2191
11/03/2009
/Wei Y Zhen/
Supervisory Patent Examiner, Art Unit 2191